perspectives libres
"Tout ce qui élève unit" Charles Péguy no. 18

La France et la mer

Perspectives Libres

N° 18 - Avril – Juin 2016

Perspectives Libres

« Tout ce qui élève unit. »
Charles Péguy

Directeur de la rédaction et de la publication :
Pierre-Yves Rougeyron

Secrétaire général :
Ambroise Marcilhacy

Comité de rédaction :
Paul de Berranger, Alain Rohou, Julien Funnaro, Philippe Arondel.

Rédaction : 38, rue Desaix - 75015 Paris
Téléphone : 06 17 69 32 93
Email : revue.libres@gmail.com
Site internet: http://www.cerclearistote.com

Abonnement : 40 euros pour 4 numéros, à l'Association des amis de la Revue Libres (ADARL)

Ont participé à ce numéro :

Jean-Marie BIETTE, Horacio CALDERON, Franck DUHAUTOY, Julien FUNNARO, Yan GIRON, Elisa HERRI, Nicolas KLEIN, Patrick LOUVIER, Clément NGUYEN, Frank PASQUALE, Jack RASMUS, Ladislas ROLLAND, Pierre-Yves ROUGEYRON, Geoffrey TILL, Lars WEDIN, Olivier ZAJEC

Une nouvelle course aux armements : surveillance des données informatiques et finance dématérialisée.

Frank PASQUALE*

A l'heure actuelle, le thème de la surveillance est sujet à controverses. De gigantesques appareils de renseignements nationaux et internationaux sont apparus en Europe, en Amérique du Nord et en Asie. Ils commettent parfois des erreurs spectaculaires, ignorant des menaces réelles ou, à l'inverse, stigmatisant et jetant en prison des personnes innocentes. Les services de renseignement ont alors tendance à mettre leurs échecs sur le compte de l'insuffisance des moyens de surveillance. D'après eux, si l'on pouvait avoir accès à de plus grandes réserves de données, et de manière plus immédiate, on serait alors capable de détecter, de prévenir et de mettre en échec davantage de menaces.

Quand de tels moyens de surveillance sont demandés, l'on observe que certaines franges de la société ont la possibilité de mobiliser des ressources en vue de s'y opposer, tandis que d'autres ne le peuvent pas. En voici un

* **Frank Pasquale,** professeur de droit à l'Université du Maryland, est un spécialiste des technologies de l'information et des problématiques qu'elles suscitent sur le plan social et juridique. Dernier ouvrage paru : *La Société de la boîte noire : les algorithmes secrets qui contrôlent l'argent et l'information* (2015).

exemple : une fraude commise aux Etats-Unis par des *membres du personnel médical* a eu pour conséquence de déclencher une enquête à grande échelle basée sur des données très importantes qui a mobilisé à la fois les secteurs publics et les secteurs privés dans le but de vérifier les demandes de remboursement des médecins et des hôpitaux[1]. Mais la surfacturation des compagnies d'assurance privées a été à peine prise en compte par le Ministère de la Santé et des Services aux Personnes[2]. Les assureurs, plus nombreux et plus puissants politiquement, peuvent contourner la surveillance minutieuse et les sanctions que doivent endurer de plus petits prestataires médicaux.

Le même deux poids deux mesures s'applique *a fortiori* avec les particuliers. Il y a environ 5 ans, je parlais à une amie agée de 40 ans qui gagnait à l'époque environ 13 000 dollars par an. Elle vivait chez elle avec ses parents handicapés, et s'occupait beaucoup d'eux, tout en donnant une vingtaine d'heures de cours particuliers par semaine. J'ai appris qu'elle n'avait pas d'assurance maladie et je lui ai vivement conseillé de se renseigner sur la couverture offerte par *Medicaid* ou par les mutuelles qui permettent de couvrir des situations difficiles comme la sienne. Elle m'a répondu qu'elle l'avait fait, mais qu'elle ne remplissait pas les conditions requises : on avait regroupé ses revenus, son patrimoine ainsi que ceux de ses parents dans le cadre d'un ménage unique, et ils s'étaient avérés trop riches pour pouvoir prétendre aux prestations. « Je me demande si tu ne pourrais pas fabriquer deux boîtes aux lettres avec deux adresses différentes et installer un rideau séparant ta chambre et ta salle de bain du reste de la maison, et déclarer que tu ne vis pas avec eux... » J'avais proposé ces pistes en essayant de l'aider, ce à quoi elle me rétorqua avec un drôle de regard : « Mais ça, ça ne s'appelle pas de la fraude ? » En effet, c'est sans doute le nom qu'il convient de donner à ce que je proposais, et une nouvelle technologie de recueil de données l'aurait probablement vite découvert.

[1] Note du Traducteur : Nous avons choisi d'offrir au lecteur francophone une traduction en français de titres d'articles et de livres non traduits en français à notre connaissance. Nous pensons en effet que la traduction de ces titres, qui n'engage que nous, peut aider le lecteur dans la compréhension des débats dont il est question dans ce texte. Pasquale, « Le rôle des homologateurs privés et des députés dans la couverture médicale américaine » Revue du Droit de la Caroline du Nord (2014) « Private Certifiers and Deputies in American Health Care », *North Carolina Law Review* (2014), URL : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2473634.

[2] GAO (Cours des Comptes américaine), « Des améliorations substantielles sont attendues de la part des Centre de Services Médicaux pour recouvrer des sommes substantielles correspondant à des paiements indus ». « Fundamental Improvements Needed in CMS's Effort to Recover Substantial Amounts of Improper Payments », URL : http://www.gao.gov/assets/680/676441.pdf

Comparez le destin de mon amie avec celui des habitants de la résidence *One Hyde Park* (OHP) à Londres, complexe immobilier parmi les plus luxueux au monde. On y vend des appartements pour plus de 200 millions de dollars, lesquels sont achetés, vendus et réassemblés selon des méthodes que l'on qualifiera d'« hétérodoxes ». Il se peut d'ailleurs que quelques-uns seulement soient réellement habités : il est désormais habituel que les grandes fortunes placent leur argent dans des résidences immobilières qu'ils n'occupent guère que quelques jours à l'année sinon jamais. Et non seulement ils n'habitent pas dans ces appartements mais il est en outre fort possible qu'ils ne les possèdent même pas directement. Sur les soixante-seize appartements OHP vendus début 2013, soixante-quatre appartenaient à des noms de sociétés pour la plupart situées dans des pays comme le Liechtenstein ou encore l'Ile de Man. Les directeurs de ces sociétés peuvent en être les vrais responsables ou non. Il se peut que ces directeurs soient en réalité des conseils constitués de manière légale (ou bien encore un simple prête-nom mis là par on ne sait quel service) et qui ont contracté dans un autre pays leur droit de voter en conseil d'administration comme ils l'entendaient. Nicholas Shaxson, un des meilleurs journalistes à avoir enquêté sur la face cachée de la richesse mondiale affirme au sujet des locataires de *One Hyde Park* : « Nous pouvons conclure au moins deux choses avec certitude : ils sont extrêmement riches et la plupart d'entre eux ne veulent pas que vous sachiez qui ils sont ni comment ils ont gagné leur argent[3]. »

Ainsi, pendant que la vie des moins aisés est sous le contrôle permanent des gouvernements, une hyper-classe peut, quant à elle, cacher des propriétés parfois gigantesques et des transactions financières aux autorités fiscales (et à d'autres curieux). Remarquez aussi comme les machinations de type *One Hyde Park* contribuent à favoriser ces organismes de surveillance qui ont refusé à mon amie l'accès à une couverture médicale. Les pays perdent

[3] Nicholas Shaxson, « Une Histoire des deux Londres », « A Tale of Two Londons », *Vanity Fair*, avril 2013, ULR : http://www.vanityfair.com/society/2013/04/mysterious-residents-one-hyde-park-london.

des dizaines voire des centaines de milliards de dollars chaque année du fait de l'évasion vers des paradis fiscaux. Les déficits budgétaires qui en résultent sont une des raisons pour lesquelles il semble qu'il n'y ait jamais assez d'argent pour les programmes sociaux. Le contournement de la taxation par les fonds d'investissement des plus fortunés a pour conséquence directe une surveillance accrue sur les bénéficiaires des prestations sociales.

Cependant, alors que beaucoup de groupes de réflexion fondés par des grandes fortunes osent affirmer qu'ils luttent pour un « droit universel à la vie privée », le degré d'intimité dont jouissent les plus riches n'a que peu à voir avec celui accordé aux moins fortunés. On peut même dire que l'un est à l'inverse de l'autre. Les plus riches peuvent utiliser la loi pour maintenir secrètes leurs affaires. Or ces efforts privent l'Etat de fonds et le contraignent à surveiller et à contrôler les plus pauvres de manière toujours plus intense, dans le but d'éradiquer la « fraude aux prestations sociales », ou, choix plus simple, de maintenir ses finances à coup d'amendes. Le Ministère américain de la Justice a fourni un rapport détaillé de ce type de mécanismes au cours d'une affaire qui s'est tenue à Ferguson, dans le Missouri : du fait de recettes fiscales générales en baisse (recettes basées, pour une grande part, sur des revenus supérieurs à la moyenne), des municipalités comme celle de Ferguson ont réglé à leur façon les phénomènes de « délinquance financière », en obtenant sous forme d'amendes ce qu'elles n'avaient pas reçu en taxes. Pour saisir encore plus d'argent par ce moyen, la police devait exercer une surveillance toujours plus accrue sur une population majoritairement afro-américaine : elle jetait en prison des citoyens pour des délits mineurs et les forçait ensuite à payer pour qu'ils puissent retrouver leur liberté.

Une réforme de la justice pénale américaine a été mise en œuvre pour contrecarrer de telles pratiques. Elle risque cependant d'être détournée du fait des intérêts des plus fortunés, dont l'avarice a contribué à orienter la surveillance vers un contrôle minutieux des populations les plus pauvres en première intention. Une célèbre proposition de loi du Congrès américain, élaborée en vue de réduire les sanctions pénales pour des délits à caractère non violent, a été rédigée de façon à rendre bien plus difficile l'application de la Loi fédérale pour poursuivre en justice les criminels en col blanc. Et plus ces poursuites seront difficiles à mener, moins ceux qui en ont la charge seront motivés pour ne serait-ce que surveiller et comprendre des opérations financières complexes comme celle se cachant derrière *One Hyde Park*, ou encore derrière une kyrielle de juridictions américaines impénétrables (comme celles du Delaware, du Nevada et du Wyoming, où il est de notoriété publique que l'opacité règne en maître).

La vie quotidienne du citoyen moyen s'organise chaque jour davantage autour des exigences de ce que Shoshanna Zuboff appelle « le capitalisme de la surveillance » : un contrôle allant jusqu'à l'intimité de nos vies quotidiennes en vue d'exploiter au maximum notre potentiel de travailleurs et de consommateurs. A ce sujet, Zuboff rapporte les propos d'un responsable scientifique des données d'une société de la Silicon Valley : « Notre but ultime est de changer le comportement actuel des personnes sur une grande échelle. Quand les gens utilisent notre application, nous pouvons saisir leurs comportements, identifier les bons et les mauvais comportements et développer des manières de récompenser les bons comportements et de punir les mauvais. Nous pouvons évaluer la praticité de nos outils pour eux et leur profitabilité pour nous[4] ». Ce type de contrôle et d'influence pourrait-il être un jour soumis aux puissants ? Le voulons-nous ? Et, si c'est d'ores et déjà faisable, est-il juste qu'il ne soit pas d'ores et déjà appliqué à tous ?

Pourtant, ce qu'il y a de plus urgent à faire dans le cadre d'une réforme de la justice pénale, ce n'est pas de relâcher cette surveillance par laquelle le gouvernement a la mainmise sur les citoyens. L'urgence, c'est de savoir comment utiliser le *Big Data* pour promouvoir des formes de contrôle social susceptibles de juguler l'influence néfaste de flux financiers actuellement « hors de contôle ». Appréhender les enjeux du *Big Data* pour la vie privée dans cette perspective politique nous aide à mieux comprendre l'une des controverses relatives à la loi sur les protections des données parmi les plus médiatisées durant la dernière décennie : le refus d'Apple de développer un outil qui était censé aider le FBI à décoder des données cryptées dans un iPhone.

Nos propres systèmes de surveillance

Les révélations faites par Edward Snowden en 2013 ont constitué un tournant décisif dans l'histoire de la surveillance. Même si des journalistes et

[4] Nicholas Shaxson, Shoshana Zuboff, « Les Secrets du capitalisme de contrôle », « Surveillance Capitalism », Frankfurter Allgemeine Zeitung, 13 mai 2016, ULR : http://www.faz.net/-gsf-8eaf4

des universitaires avaient été avertis de manière individuelle de l'aide importante du secteur privé dans des activités d'espionnage illégal avant 2013, les intérêts en jeu constituaient un problème marginal. Une action prêtant à controverse, la violation de la sécurité de la NSA par Edward Snowden, un entrepreneur privé, a transformé le débat public : ces fuites ont révélé toute une documentation interne qui concernait à la fois une coopération pleinement consciente des géants des hautes technologies et des communications avec l'Etat et un fonctionnement par simple cooptation de leurs réseaux. L'interdépendance forte régnant entre l'Etat et le marché, déjà manifeste pour les opérateurs téléphoniques, est devenu difficile à ignorer pour des sociétés comme Google, Apple, Facebook, Amazon, ou encore d'autres sociétés de secteurs technologiques comparables.

Pour regagner la confiance de l'utilisateur, Google et Apple ont pris des mesures pour rendre difficile l'espionnage de leurs réseaux et de leurs systèmes. Et ainsi que l'ont déclaré les avocats d'Apple dans l'un de leur dossiers, cela « inclut un dispositif qui, s'il vient à être activé, efface automatiquement les données chiffrées après dix tentatives incorrectes de rentrer le mot de passe.[5] » Le cœur du conflit opposant Apple au FBI consiste dans le fait de savoir si, conformément au *All Writs Act*[6], le FBI peut contraindre Apple à créer des logiciels capables de désactiver la fonction autodestructive ainsi que d'autres éléments de sécurité du même ordre.

D'un strict point de vue légal, la question de la prérogative du FBI est une problématique très proche[7]. Dans la pratique cependant, un consensus différent apparaît : afin de protéger la vie privée et la sécurité sur internet en général, il ne faut pas forcer Apple à créer un tel logiciel. C'est une pente glissante et périlleuse que celle menant à la possibilité d'un décryptage généralisé sur ordre de justice : c'est la porte ouverte à une récupération immédiate de ces données par des pirates informatiques ou par des gouvernements étrangers. J'ai déjà vu cet argument sortir de l'esprit d'un ancien chef de la CIA et de la NSA (Michael Hayden), et de celle d'une commissaire de la FTC (Commission Fédérale du Commerce), Julie Brill, ou encore de celles de nombreux universitaires ainsi que d'une association de défense de la vie privée. Je comprends qu'il soit tentant de penser ainsi, en particulier si l'on s'engage avant toute autre chose dans un combat contre l'indifférence croissante de la police américaine pour le 4e Amendement et les valeurs qui lui sont liées, ainsi que dans un combat contre la violation des données par les pirates informatiques.

[5] Dossier de la défense d'Apple, pièce jointe au plaidoyer, 25 février 2016, URL : https://assets.documentcloud.org/documents/2722199/5-15-MJ-00451-SP-USA-v-Black-Lexus-IS300.pdf.

[6] Le *All Writs Act* est un amendement datant de 1789 et confédérant un pouvoir illimité à toute autorité fédérale pourvue d'une mandat de perquisition (ndlr)

[7] Orin Kerr, « Idées préalables au sujet de l'injonction concernant l'iPhone d'Apple dans l'affaire de San Bernardino : 2e Partie, le All Writs Act » « Preliminary thoughts on the Apple iPhone order in the San Bernardino case: Part 2, the All Writs Act », *Washington Post: Volokh Conspiracy* (blog d'Eugène Volokh), 19 février 2016, ULR : https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/19/preliminary-thoughts-on-the-apple-iphone-order-in-the-san-bernardino-case-part-2-the-all-writs-act/.

D'un autre côté, le Président Obama a eu les mots suivants : « Vous ne pouvez pas adopter une vision absolutiste sur ce sujet. Si votre argument consiste à vouloir encoder tout et n'importe quoi et à créer des sortes de boîtes noires, puisque c'est désormais possible, cela revient à faire de nos téléphones des fétiches qui se trouvent placés au-dessus de toute autre valeur[8]. » David Golumbia, lui, a fortement remis en cause la position douteuse d'Apple[9]. Nathan Newman, enfin, a montré qu'un cryptage indéchiffrable pouvait être utile dans un certain nombre de situations pour le moins troublantes.

Un procès pour évasion fiscale impliquant des responsables importants de la banque suisse UBS a souligné combien le chiffrage des données pouvait entraver les enquêtes fiscales. A cette occasion, des témoins ont rapporté par le détail de quelle manière les banquiers cachaient les données sensibles d'un client dans des onglets du jeu du « Solitaire », lui-même situé dans un lecteur secret d'un ordinateur portable protégé par un mot de passe, ou encore dans des codes informatiques avec mots de passe à utiliser en situation d'urgence, de telle sorte que toutes les données concernant une activité illégale soient éliminées de manière instantanée.

[8] Barack Obama, *Conférence au Festival South by Southwest Interactive*, 11 mars 2016, ULR : https://www.whitehouse.gov/the-press-office/2016/03/14/remarks-president-south-southwest-interactive

[9] David Golumbia, « Les portes dérobées sont-elles réelles ou virtuelles ? Sur la logique défectueuse de l'affaire opposant Apple au FBI » « Are « Backdoors » Real or Virtual ? The Logical Flaw in #AppleVsFBI », 25 février 2016, ULR : http://www.uncomputing.org/?p=1708

Rien qu'au mois de mai dernier, lorsque les autorités fiscales québécoises ont perquisitionné les bureaux d'Uber Canada, des ingénieurs depuis les bureaux d'Uber à San Francisco sont parvenus à chiffrer à distance des données conservées au Canada. Les enquêteur du fisc voulaient savoir si la société fraudait sur la TVA locale mais au moment d'étudier les données de la compagnie, conformément au mandat judiciaire, ils se sont aperçu que les systèmes étaient verrouillés [...]. Le chiffrage inviolable des données est [...] une fausse solution, un bidule technologique dont, en termes aussi bien de criminalité, de terrorisme que d'infractions fiscales, les effets pervers en viendront à en dépasser les bénéfices[10].

Les défenseurs de la vie privée ont raison de se montrer inquiets face à un FBI qui a déjà abusé de son autorité dans le passé et peut parfaitement recommencer dans le futur. Je suis cependant certain qu'ils se seraient contrariés qu'une grande société réussisse à chiffrer toutes les activités d'immixition dans la vie des gens grâce à une technologie comme celle développée par Apple, tout en échappant aux sanctions grâce à ce même chiffrage. Imaginez, par exemple, une application destinée à améliorer la qualité de vie du personnel d'une administration ou d'une société et qui utiliserait les montres Apple pour collecter et pour transmettre les données concernant la santé de l'utilisateur[11]. C'est la porte ouverte à tous les abus, par exemple à une discrimination des employés malades ; abus d'autant plus faciles à réaliser que les transferts des données seraient faits à l'insu de tous, sauf de ceux qui en sont les instigateurs[12].

[10] Nathan Newman, « Déverrouillage de l'iPhone de San Bernardino : justice sociale et vie privée en question » « The Social Justice and Privacy Case for Unlocking the San Bernardino iPhone », *Huffington Post*, 26 février 2016, ULR : http://www.huffingtonpost.com/nathan-newman/the-social-justice-and-privacy_b_9328118.html

[11] Ifeoma Ajunwa, Kate Crawford, and Jason Schultz, « Le contrôle illimité des travailleurs » « Limitless Worker Surveillance» , *Revue californienne du Droit California Law Review*, ULR : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746211

[12] Frank Pasquale, « L'Autre Big Brother » « The Other Big Brother », *The Atlantic*, 21 septembre 2015, ULR : http://www.theatlantic.com/business/archive/2015/09/corporate-surveillance-activists/406201/; Jana Kasperkevic, « Programmes de mieux-être au travail : votre patron, espion de votre santé ? » « Wellness Programs at Work : Could Your Boss be Spying on your Health? », *The Guardian*, 29 février 2016, ULR : https://www.theguardian.com/business/2016/feb/29/wellness-programs-boss-spying-on-your-health

La course aux armements cryptographiques

Beaucoup d'observateur ont été surpris lorsque l'ancien chef de la NSA et de la CIA Michael Hayden est intervenu en plaidant contre le FBI[13]. Selon lui, « l'Amérique est simplement plus sûre avec un encodage totalement inviolable ». Mais il convient de remarquer ici que par « inviolable », il n'entend pas « inviolable par quiconque ». En réalité, son souhait est que la NSA demande une rallonge budgétaire afin qu'elle puisse embaucher des cryptographes capables de pirater les téléphones Apple. D'autres personnes affirment d'ailleurs que la NSA est déjà en mesure de pirater un téléphone par ses propres moyens[14].

Cependant, la thèse de Hayden semble se résumer à un problème de compétences institutionnelles. Puisqu'il considère que la NSA est l'organisation à même de traiter tout ce qui a trait à Internet, il souhaite qu'elle poursuive dans la voie d'une course aux armements cryptographiques contre des sociétés aussi importantes qu'Apple[15]. Il se moque des défenseurs des libertés civiles qui avaient lutté contre la puce Clipper[16] dans les années 1990, étant donné que, d'après lui, on avait contourné le problème avec l'accroissement des potentialités de collecte massive. Il pense manifestement que la NSA

[13] Susan Page, « Un ancien chef de la NSA soutient Apple dans l'affaire des portes dérobées de l'iPhone » « Ex-NSA Chief Backs Apple on iPhone « Back Doors » », *USA Today*, February 21, 2016, ULR : http://www.usatoday.com/story/news/2016/02/21/ex-nsa-chief-backs-apple-iphone-back-doors/80660024/

[14] Tom Ashbrook, « Apple, le FBI et votre vie privée » « Apple, the FBI, and Your Privacy », *NPR: On Point*, 1er mars 2016, ULR : http://onpoint.wbur.org/2016/03/01/apple-fbi-san-bernardino-encryption

[15] Andrew Nusca, « Un ancien chef de la NSA au cœur de l'affaire Apple contre le FBI : beaucoup de membres importants de l'Etat soutiennent Apple » « Ex-NSA Director : In Apple vs. FBI, Many Top Gov't Officials Side with Apple », *Fortune*, 19 février 2016, , ULR : http://fortune.com/2016/02/19/hayden-apple-fbi/

[16] NdT : « La puce Clipper - ou Clipper chip était un projet de cryptoprocesseur conçu par la NSA durant les années 1980. Elle fut développée dans le cadre d'un projet de l'administration américaine destiné à doter les appareils électroniques vendus au grand public d'une puce de sécurité » - Wikipédia.

aura toujours l'avantage et ce, quels que soient les outils de codage inventés par les entreprises. Et quiconque connaît la facilité avec laquelle les données sont partagées par les services de l'Etat américain, ainsi que le montre Bernard Harcourt dans son livre *Exposed*, est capable d'anticiper la suite : à la suite des recommandations émanant du rapport final rédigé par la commission sur le 11 septembre, le FBI continuera d'abattre les cloisons entre sa collection de données et celle d'autres agences[17]. Nous savons en effet que « les données de la NSA doivent être partagées avec d'autres services de renseignement comme le FBI sans aucune forme de censure destinée à protéger la vie privée[18] ».

La course aux armes de cryptage et de décryptage envisagée non sans légèreté par Hayden me frappe aussi par son peu d'utilité. Comme Phil Rogaway l'a remarqué dans un récent essai intitulé *The Moral Character of Cryptographic Work* (*Pour une éthique cryptographique*), nous devrions être libres de nous demander :

« Et si un tel savoir informatique n'apportait rien de bon à l'homme ? Des penseurs techno-sceptiques comme Jacques Ellul, Herbert Marcuse ou Lewis Mumford voyaient les choses en ces termes : ils considéraient la technologie moderne comme un système d'emboîtement hors de contrôle qui, au lieu de satisfaire aux besoins de l'homme, engendrait des désirs vains tout en permettant la construction d'armes toujours plus anthropocides [...][19]. »

[17] *Rapport de la commission sur le 11 septembre, The 9/11 Commission Report*, ULR : http://govinfo.library.unt.edu/911/report/911Report.pdf

[18] Radley Balko, « Surprise ! Les données recueillies par la NSA vont bientôt être utilisées régulièrement dans des affaires de politique intérieure qui n'auront rien à voir avec le terrorisme ». « Surprise! NSA Data will Soon Be Routinely Used for Domestic Policing that has Nothing to do with Terror », *Washington Post*, 10 mars 2016, ULR : https://www.washingtonpost.com/news/the-watch/wp/2016/03/10/surprise-nsa-data-will-soon-routinely-be-used-for-domestic-policing-that-has-nothing-to-do-with-terrorism/

[19] Phillip Rogaway, « Morale de la Cryptographie » « The Moral Character of Cryptographic Work », décembre 2015, ULR : http://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf

D'un point de vue américano-centré, ces simulacres de guerres incessants autour des diverses tactiques de cryptage entre experts d'Apple à Cupertino en Californie et de la NSA à Fort Meade au Maryland peuvent aboutir à l'émergence d'un groupe de professionnels mieux à même de résister, par exemple, à une avalanche d'attaques cybernétiques chinoises (à propos desquelles des groupes de réflexions financés par des entreprises de haute-technologie font d'obscures prédictions)[20]. Mais les inévitables ripostes mondiales qu'engendreraient de tels développements constitueraient assurément le début d'une nouvelle course aux armements, avec des enjeux toujours plus élevés.

Un monde dans lequel le FBI doit aller à la NSA pour décrypter des données dans des iPhones pourrait être préférable à un monde où l'agence peut, *via* le *Act Writs Act*, forcer des sociétés à déchiffrer leur propre codage. Ou bien un jugement défavorable au FBI pourrait accélérer la collaboration entre les deux services (tant au plan national qu'au plan international) vers un « espace commun de partage des renseignements » plus solide qu'il ne l'est actuellement. Une victoire d'Apple dans son procès qui l'oppose au FBI ne va pas faire se dresser comme par magie un mur en cryptages protégeant chacune de nos communications[21]. Elle ne va d'ailleurs même pas l'autoriser à protéger ses informations des enquêteurs du FBI, ni encore moins lui enjoindre, dans une décision à portée jurisprudentielle, de tenir le FBI à l'écart de ces informations.

Le monde de la surveillance moderne fait s'enchevêtrer les domaines sociaux, techniques et juridiques de manière tellement complexe que chaque victoire sur le terrain judiciaire génère des contrecoups techniques et so-

[20] Thomas E. Ricks, « Tous les officiers de l'armée devraient lire le roman *La Flotte fantôme* de P.W. Singer et August Cole » « Singer and Coles « Ghost Fleet » : Every Army Officer Should Read it and It's Fun », *Foreign Policy*, June 11, 2015, ULR : http://foreignpolicy.com/2015/06/11/singer-and-coles-ghost-fleet-every-army-officer-should-read-it-and-its-fun/ « Source Watch : la Fondation pour une Nouvelle Amérique » , « Source Watch : New America Foundation », ULR : http://www.sourcewatch.org/index.php/New_America_Foundation.

[21] Emily Field, « Un membre de la Commission Fédérale des Echanges détruit la pensée magique de l'Etat dans l'affaire Apple » « FTC Official Slams Gov't Magical Thinking in iPhone Row », *Law 360*, 10 mars 2016, ULR : http://www.law360.com/articles/770115/ftc-official-slams-gov-t-magical-thinking-in-iphone-row.

ciaux, que chaque avancée technologique provoque des réponses juridiques, et ainsi de suite. Il ne s'agit pas seulement d'examiner l'immensité de l'appareil moderne de surveillance étatique, mais aussi sa relation de symbiose avec le prétendu secteur privé.

Le jeu de séduction des gentils PDG contre le méchant Etat.

Pourquoi dès lors le cas est-il devenu une « *cause célèbre* » ? Parce que les confrontations politiques actuelles se font à coup de mots-dièse, de batailles juridiques et de décisions de justice de très grande portée. L'affrontement des partis devant un juge et bien plus amusant et facile à suivre que ces byzantines politiques bureaucratiques qui régulent la circulation des flux d'information entre nos innombrables services de renseignements, de police et de sécurité[22]. Il n'est guère populaire de soutenir le FBI, étant données ses actions répétées de surveillance d'activités pourtant protégées par le Premier Amendement[23]. Et pendant ce temps, il se peut que les citoyens soutiennent les positions défendues par Apple devant la justice avec le même enthousiasme qu'ils adoptent ses appareils. L'ouvrage de Bernard Harcourt, *Exposed*, décrit combien cet engagement peut devenir passionné :

« C'est tout à fait volontairement et non sans fierté que nous attachons à notre poignet un véritable appareil de contrôle, la montre Apple. Nous l'exhibons même. Assurément, l'Etat n'a plus besoin d'imposer par contrainte le port d'un bracelet électronique, alors que c'est avec tellement d'enthousiasme que nous attachons à notre propre poignet ce fascinant objet lisse. Et c'est ainsi que le coeur rempli de joie, de bonheur et d'enthousiasme, nous la portons sur notre propre corps, tel un second corps social venant recouvrir le premier. Et certes, nous pouvons l'affirmer : la montre intelligente a remplacé le bracelet électronique[24]*. »*

Prendre parti dans ce que les réseaux sociaux appellent la controverse « #ApplevFBI » peut réduire en nous la dissonance cognitive liée à l'émergence de relations sociales chaque fois plus soumises aux féodalités que sont à la fois les géants de la technologie et les structures profondes de l'Etat[25] : faire confiance à l'Etat pour nous protéger du terrorisme ou faire confiance à Apple pour protéger nos données puis, comme d'habitude, commenter sur Tweeter, Instagram, Snapchat, Facebook...

Mais toute nouvelle solution amène de nouveaux problèmes. Songez aux leçons que l'on peut tirer du bracelet électronique, une solution bon marché à l'incarcération de masse[26]. Alors, certes, en démocratisant une forme parfaite de maison d'arrêt portative, on a pu laisser hors de prison des dizaines de milliers de personnes. Mais de l'utilisation du bracelet électronique dans le but de faire baisser les coûts de la surveillance et du contrôle de ceux qui auraient été autrefois emprisonnés, à son utilisation (ou l'utilisation d'une technologie similaire) comme mode d'identification, de contrôle et de surveillance de populations entières indépendamment de toute décision de justice, il n'y a qu'un pas. Dans ce contexte, la technologie relève à la fois du rêve et du cauchemar : c'est seulement grâce à la numérisation qu'on a pu réduire le taux d'emprisonnement, celle-là même qui permet que chaque aspect de notre « société de contrôle » deleuzienne nous devienne une entrave, soit une prison virtuelle soit une information potentiellement exploitable par un tiers[27].

Dans le conflit opposant Apple au FBI, un dilemme de complexité similaire se pose. Rendus méfiants à l'égard des autorités policière et se tenant sur leurs gardes quant aux méthodes habituelles dont ils les tiennent responsables, de plus en plus d'Américains veulent que leurs communications soient protégées technlogiquement. La mise en commun d'un logiciel libre de cryptage, appelée de ses vœux par Rogaway, ne s'étant pas matérialisée, ils

[22] *Washington Post,* « L'Amérique classée Secret Défense » « Top Secret America », ULR : http://projects.washingtonpost.com/top-secret-america/.
[23] *ACLU,* « La liberté de parole sous contrôle » « Policing Free Speech », 11 août 2010, ULR : https://www.aclu.org/files/assets/policingfreespeech_20100806.pdf.
[24] B. E. Harcourt, *Mise à nu : Désir et désobéissance à l'ère du numérique. Exposed: Desire and Disobedience in the Digital Age* (2015)

[25] Bruce Schneier, « Une sécurité féodale » « Feudal Security », ULR : https://www.schneier.com/blog/archives/2012/12/feudal_sec.html ; Mike Lofgren, « *Les Structures profondes de l'Etat : chute de la Constitution et avènement d'un gouvernement fantôme ».» The Deep State: The Fall of the Constitution and the Rise of the Shadow Government* » (2016).
[26] Hadar Aviram, « *La Braderie du crime : la politique en période de récession et la transformation du châtiment aux Etats-Unis » « Cheap on Crime: Recession-Era Politics and the Transformation of American Punishment* » (2015).
[27] Jathan Sadowski and Frank Pasquale, The Spectrum of Control: A Social Theory of the Smart City, *First Monday*, July 6, 2015, ULR : http://firstmonday.org/ojs/index.php/fm/article/view/5903/4660.

placent leur confiance dans un géant de l'économie[28]. Qui d'autre dans le monde pense de la sorte ? Par quels moyens responsabilise-t-on Apple et l'empêche-t-on de trahir les utilisateurs de ses produits ? Existe-t-il des formes de cryptage qui rendraient une telle responsabilité sujette à controverses ? Ou, pour reprendre la question posée par Jürgen Gueuter : « Alors qu'à l'échelle du monde, sommes reliés les uns aux autres et que nous vivons dans des sociétés connectées et interdépendantes, comment pouvons-nous définir les relations entre des multinationales d'un côté et les lois que nous avons créés de l'autre[29] ? »

Certains services au sein du gouvernement américain soutiennent le développement de la technologie du cryptage, tandis que d'autres l'attaquent, et d'autres encore adoptent les deux positions[30]! De grosses sociétés comme Apple comprennent maintenant l'avantage commercial qu'elles peuvent tirer de lutter contre des exigences de décryptage aux Etats-Unis, alors qu'elles sont prêtes à répondre positivement lorsque des exigences similaires sont émises par l'administration chinoise[31]. Aussi longtemps que nos « bénéfices tirés des investissements dans le domaine de la surveillance dériveront en

[28] Phillip Rogaway, « Morale de la Cryptographie » « The Moral Character of Cryptographic Work », décembre 2015, ULR :
http://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf

[29] Jürgen Geuter, « La Liberté, un iPhone et le refus de penser en termes politiques » « Liberty, an iPhone, and the Refusal to Think Politically », *Boundary2*, 18 février 2016, ULR :
http://www.boundary2.org/2016/02/liberty-an-iphone-and-the-refusal-to-think-politically/.

[30] Yasha Levine, « Presque tous ceux impliqués dans le développement de Tor ont été (ou sont) financés par l'Etat américain ». « Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government », *Pando*, July 16, 2014, https://pando.com/2014/07/16/tor-spooks/; Damian Paletta, « Comment l'Etat américain combat le cryptage tout en contribuant à son développement » « How the US Fights Encryption and also Helps Develop It », *Wall Street Journal*, 22 février 2016, ULR :
http://www.wsj.com/articles/how-the-u-s-fights-encryptionand-also-helps-develop-it-1456109096.

[31] David Pierson, « Pendant qu'il défie l'Etat américain, Apple se plie aux ordres chinois et en récolte de grosses récompenses » « While it Defies U.S. Government, Apple Abides by China's Orders, and Reaps Big Rewards », *Los Angeles Times*, 26 février 2016, ULR : http://www.latimes.com/business/technology/la-fi-apple-china-20160226-story.html.

premier lieu, sinon entièrement, des [...] marchés en regard des comportements futurs », nous pouvons nous attendre à ce que tant les entreprises que les gouvernements continuent à jouer un tel double jeu : exercer un contrôle toujours plus fort sur nos vies tout en affirmant protéger notre vie privée dans le même temps, cogner sur le cryptage dans certains contextes, alors qu'on le renforce dans d'autres[32]. Eric Schmidt va présider non seulement le tout nouveau Conseil Consultatif de l'Innovation pour la Défense (*Defense Innovation Advisory Board*), qui dépend du Ministère de la Défense, mais il va aussi diriger une société de portefeuilles possédant une participation financière dans une entreprise qui s'était déclarée « indignée » par la NSA, organisme qui dépend lui aussi du Ministère de la Défense, et il présidera enfin le conseil d'une fondation qui s'offre de proposer une expertise impartiale sur cette très grande controverse[33].

Deux problèmes, une réponse.

L'ouvrage de Loïc Wacquant paru aux Etats-Unis sous le titre *Punishing the Poor: The Neoliberal Government of Social Insecurity* (*Punir les moins aisés : le gouvernement néolibéral de l'insécurité sociale*) affirme que l'« hyperinflation » de la population carcérale aux Etats-Unis résulte d'un changement d'axe dans la politique de l'Etat où l'on passe de la promotion de la sécurité économique à la promotion de la sécurité physique par le biais d'une politique de « tolérance zéro », y-compris pour les délits non violents[34]. Selon Wacquant, les médias et les autorités politicières font équipe

[32] Shoshana Zuboff, « Les Secrets du capitalisme de contrôle » « Surveillance Capitalism, » Frankfurter Allegemeine, 13 mai 2016, ULR : http://www.faz.net/-gsf-8eaf4

[33] David Goldman, « Eric Schmidt est embauché au Pentagone » « Eric Schmidt Gets a Job at the Pentagon », *CNN Money*, 2 mars 2016, ULR :
http://money.cnn.com/2016/03/02/technology/eric-schmidt-pentagon/ ; « Affaire Snowden : Google « s'indigne » du piratage attribué à la NSA » « Snowden Leaks : Google « Outraged » at Alleged NSA Hacking », *BBC News*, 31 october 2013, http://www.bbc.com/news/world-us-canada-24751821 ; « Présentation de la Fondation pour une Nouvelle Amérique » « Company Overview of New America Foundation », *Bloomberg*,
http://www.bloomberg.com/research/stocks/private/board.asp?privcapId=49437705.

[34] Kim Phillips-Fein, « Le Dilemme du prisonnier » « Imprisoner's Dilemma », *Book Forum*, septembre, octobre, novembre 2009,
ULR : http://bookforum.com/inprint/016_03/4332.

pour « mettre en scène [...] un théâtre criard de morale civique sur la scène duquel les élites peuvent jeter en pâture à l'opinion des figures déviantes [...] et contrebalancer ainsi le déficit de légitimité dont ils souffrent quand ils renoncent à leur mission de protection sociale et économique une fois au pouvoir[35] ». De même que certains experts en anti-terrorisme fustigent le « théâtre sécuritaire », Wacquant conclut de son analyse du système pénal qu'il va bien au-delà de ses objectifs déclarés d'assurer la sécurité aux citoyens vertueux[36]. Selon lui, ce système tend à devenir « autophage » en vertu de sa brutalité intrinsèque : il se renouvelle sans cesse dans un cycle de récidive, d'insécurité croissante et de mesures de répression de plus en plus importantes. Comme la théorie sociale des « systèmes autopoïétiques » de Niklas Luhmann, qui se constituent et se reconstituent eux-mêmes selon une logique interne qui peut avoir peu à voir avec la santé générale ou le bien-être de la société[37], la théorie de la « sanction néolibérale » de Wacquant met en garde sur le fait que la généralisation de la surveillance peut constituer un processus détaché de la réalité des problèmes de sécurité.

Si la surveillance généralisée n'est pas prête de disparaître, le meilleur moyen de résoudre les problèmes soulevés par Wacquant est de la rendre « équitable » en ne la centrant pas uniquement sur les « moins favorisés » mais aussi sur les particuliers les plus puissants[38]. Les accusations de liens coupables entre le monde de l'entreprise et l'administration sont devenus un

[35] Loïc Wacquant, *Punir les moins aisés : le gouvernement néolibéral de l'insécurité sociale, Punishing the Poor: The Neoliberal Government of Social Insecurity* (2009)

[36] John Mueller, *L'Exagération : Comment les hommes politiques et les entreprises de lutte contre le terrorisme gonflent les menaces pesant sur la sécurité nationale et pourquoi nous les croyons, Overblown : How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them* (2006).

[37] David Seidl and Dennis Schoeneborn, « La théorie autopoïétique des organisations de Niklas Luhmann : apports, limites et perspectives d'avenir » « Niklas Luhmann's Autopoietic Theory of Organisations: Contributions, Limitations, and Future Prospects », 1er février 2010, ULR : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1552847. Note : Teubner prête à Luhmann le travail de Scheuerman, dans le dernier chapitre.

[38] Les études de Larry Cata Becker sur la loi Sarbanes-Oxley, perçue comme un mécanisme de surveillance, ont montré qu'elle constituait une bonne illustration de pratiques qui devraient être étendu à un contrôle en temps réel. Le projet de Jaron Lanier de « pratiques financières structurées » devrait contribuer à ce processus. Sheldon Wolin, « La Démocratie Entreprise » « Democracy Incorporated » (2010).

lieu commun en politique[39]. Elles ont contribué à une baisse de confiance durable du citoyen envers l'Etat. Pourtant, au moment même où les citoyens se méfient de plus en plus du personnel étatique, la crainte du terrorisme les a rendus de plus en plus dépendants de l'appareil de sécurité nationale. A une époque où l'on réduit fortement le budget nécessaire pour mener à bien les programmes sociaux, les dépenses pour soutenir les initiatives militaires, renforcer la sécurité nationale et subvenir aux besoins des autorités policières continuent de croître[40]. Il est difficile, voire conceptuellement impossible, d'estimer le balance des coûts et des bénéfices de ces investissements inédits dans la militarisation et dans la surveillance. Cependant, une surveillance asymétrique menace de porter à un autre niveau la méfiance envers l'Etat, ébranlant par là-même les relations de coopérations entre l'Etat et le citoyen qu'elles sont censées cultiver.

Les Etats-Unis ont dû affronter deux crises majeures durant la première décennie du XXI*ème* siècle : les attentats de New-York et de Washington en septembre 2001 et le risque d'effondrement de son système financier en septembre 2008. Pour ce qui concerne le 11 septembre, le pays a conclu qu'il avait fait une erreur catégorielle à propos du type de menaces posé par le terrorisme. Les Etats-Unis avaient compté sur un mode de coopération relevant de l'improvisation entre les spécialistes de l'Administration Fédérale de l'Aviation, les effectifs policiers au niveau local et les compagnies aériennes dans le but de prévenir les détournements d'avion. Estimant qu'au pire le fait de détourner un avion ou de le faire exploser tuerait les passagers à bord, les membres du gouvernement pensaient que les autorités nationales, locales et privées disposaient de moyens suffisants investis à un niveau optimal dans la dissuasion. Jusqu'à l'attentat, aucune personnalité de premier ordre au sein de l'appareil étatique n'avait vraiment réfléchi à l'hypothèse d'un avion utilisé comme une arme pouvant tuer des dizaines de milliers de civils.

Après les attentats, les services de renseignement et le Ministère de la Sécurité Intérieure ont recentré leurs efforts pour mieux contrôler les menaces affectant le pays. Ils ont développé une véritable industrie dédiée à la surveil-

[39] *Encyclopédie de la politique américaine, Encyclopedia of American Politics,* entrées à *Capture. Cronyism. Corruption. Influence Peddling.*

[40] Harcourt, *La Sanction néolibérale, Neoliberal Penality*; Louis Wacquant; *Texas à la dure, Texas Tough* ; comparaison des règles émanant du Bureau du Budget du Congrès Américain (*Congressional Budget Office*) CBO qui encadre les réformes de santé et de leur absence pour ce qui concerne les dépenses militaires.

lance de personnes et de groupes à risque. L'Etat a considérablement renforcé ses capacités de surveillance dans sa traque aux terroristes. Le Ministère de la Sécurité Intérieure et les services de renseignement ont tous les deux collaboré avec des agents de la force publique à un niveau local et des entreprises privés de grande importance stratégique. Les services fédéraux rassemblent des renseignements en collaboration avec l'Etat et des autorités policières locales dans ce que le Congrès a appelé la « Plateforme d'Echanges de Renseignements » sous le sigle ISE (« Information Sharing Environment »)

Nous n'avons pas vu un niveau similaire de restructuration et de renforcement de la surveillance dans le domaine de la finance - que ce soit à Wall Street ou dans les sphères plus étroites de l'évasion fiscale telle qu'abordée dans cet article. Bien qu'une soudaine destabilisation des marchés financiers ou que la lente hémorragie des revenus fiscaux fassent peser une menace sur la sécurité nationale, les Etats-Unis n'en sont qu'aux balbutiements dans la création d'une nouvelle Plateforme d'Echanges de Renseignements qui concernerait la finance. Etant donné le formidable défi posé par la finance numérisée et mondialisée, il peut être nécessaire d'envisager une coordination bien plus étroite entre les différents acteurs afin de lutter contre l'instabilité financière. Le Pentagone a déjà « simulé ce qui se passerait si le monde en venait à se désagréger dans une série de véritables guerres financières[41] ». Seulement, on ne devrait pas se contenter de jouer à la guerre avec ces scénarios mais aussi mettre en pratique une surveillance approfondie des flux des marchés et des mouvements de capitaux.

Le président de la SEC, la Commission boursière américaine (*The US Securities and Exchange Commission*), a admis en 2010 que « [l]a technologie pour collecter des données et surveiller nos marchés a souvent jusqu'à deux décennies de retard sur la technologie actuellement en usage par ceux que nous sommes chargés de réguler[42] ». Beaucoup de travailleurs intellectuels se sentent « hors-jeu » lorsque leur ordinateur date de trois ans. Encore plus surprenant, ceux qui sont chargés de réguler la finance américaine ont nettement moins de ressources que les sociétés qu'ils sont censés réguler. Durant ces dernières années, le revenu annuel d'une poignée d'individus travaillant

[41] Eric Weiner, *Le Marché fantôme. The Shadow Market*, 13 (2010).

[42] Mary Schapiro, *Déclaration préliminaire à la première séance du SEC, Opening Statement at the SEC Open Meeting — Essai de contrôle renforcé*, SEC.

dans la finance éclipse le budget de services étatiques comme ceux de la SEC ou encore de la CFTC (Organe de Contrôle et de régulation des marchés financiers - *Commodity Futures Trading Commission*). Quand un simple spéculateur travaillant pour un fonds d'investissement peut gagner en une seule année plus de trois fois le budget annuel total de la SEC, la régulation relève plus de la mascarade que de la réalité[43].

Le Pentagone est déjà en train d'investir dans la cybersécurité, ce qui aidera toutes les sociétés américaines, y-compris les sociétés financières, à éviter les attaques par internet. Mais les flux financiers modernes ne sont pas uniquement menaçant parce qu'un virus informatique pourrait saboter telle transaction ou détricoter tel registre de données : ces flux sont de plus en plus incontrôlables et destabilisants par eux-mêmes, alors que tous leurs composants fonctionnent normalement. Et si jamais un cryptage indéchiffrable devait être pleinement intégré aux échanges financiers des plus fortunés, les Etats, déjà à court d'argent, pourraient voir compromises leurs capacités à lever l'impôt.

Fort heureusement, construire de manière anticipée un système d'alertes dans le système financier ne devrait pas être aussi difficile ni aussi coûteux que le gigantesque appareil de lutte contre le terrorisme. Le travail préparatoire a déjà été pour une grande part déjà effectué, tant dans son versant technique que dans son versant légal. Mais il exige la mobilisation conjointe de trois secteurs de la vie politique actuellement distincts : la sécurité nationale, la cybersécurité et la finance. La recherche en guerre cybernétique a déjà informé dans le passé les responsables de la sécurité nationale de problèmes de cybersécurité : les progrès technologiques militaires peuvent aussi bien être un atout qu'un poids, s'ils peuvent être piratés par des ennemis. Cependant, les experts en guerre cybernétique viennent de commencer à analyser les risques encourus par un système financier en grand désordre. Les experts financiers comprennent ces risques, mais seul un petit nombre d'entre eux ont tenté de les communiquer aux autorités militaires. De la même façon que les experts en aviation ont soit échoué à prendre conscience du danger potentiel que constitue un avion transformé en arme, soit échoué à communiquer sur ce sujet, les spécialistes du Droit des finances n'ont pas encore communiqué de manière appropriée sur la fragilité de notre système

[43] Le financier John Paulson aurait gagné plus de 4 milliards de dollars en 2008. Le budget de la SEC s'élevait à environ 1 milliard de dollars en 2008.

économique. Loin de relever uniquement des préoccupations mystérieuses d'un petit nombre de personnes, la technologie appliquée à la finance est une pierre angulaire de l'ordre social et il est temps de les considérer comme telles

Traduction : Pierre Kermorvant.

« Libres propos »